U.S. General Services Administration

Office of Governmentwide Policy

Interoperability Parameters for Trusting non-Federal Identity Cards

Judy Spencer
Chair, Federal Identity
Credentialing Committee
judith.spencer@gsa.gov

Federal Directive

- The scope of HSPD-12 is restricted to "*establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)*."
- FIPS 201 standard is "*applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.*"

Basis for PIV Card Trust

- Well-defined standards
- A compliance regimen that ensures parties adhere to the well-defined standards
- Relying Party verification that allows relying parties to verify compliance when trusting and
- Secure components inherent to the PIV Card

Proposition

- Organizations external to the U.S. Federal government have expressed a desire to establish identity credentials that are interoperable with the Federal Personal Identity Verification (PIV) card.
- They want a card that is:
  - Technically compatible/interoperable with the PIV system
  - Capable of Trust in the Federal environment

Definitions

- PIV Compatible – cards that meet the technical specifications so that PIV infrastructure elements such as card readers are capable of working with the cards, but the credential itself has not been issued in a way that assures it is trustworthy by federal relying parties.
- PIV Interoperable – cards that meet the technical standards to work with PIV infrastructure elements such as card readers and are issued in a way that allows federal relying parties to trust the cards.

Assumptions

- PIV interoperable cards will be on a smart card platform that is technically compatible with the PIV card (i.e. NIST SP 800-73)
- The card is populated in a like manner to the PIV card (as defined in FIPS 201).
- Individual card holders are employees/constituents of the issuing organization.
- Individual Federal organizations will determine the extent to which PIV-interoperable identity cards will be trusted as identity credentials within their areas of control.

Compatible Card

- Card face indicates
  - Sponsor/Issuer
  - Name
  - Affiliation
  - Expiration Date
  - First Responders
  - Citizenship
- Visually distinct

- Contactless Interface
  - CHUID
- Contact Interface
  - Card Capability
  - CHUID
  - Printed Information (optional)
  - Biometrics
    - Fingerprint Minutiae
    - Facial Image (optional)
  - Digital Certificates
    - Authentication
    - Signature (optional)
    - Key Management (optional)
    - Card Authentication (optional)
  - Security Object

Enabling Trust – What's Missing

- Identity Proofing Requirements
  - Non-federal entities cannot satisfy FIPS 201 requirements
  - Federal suitability requirements to not apply
- Unique Identifier
  - Non-federal entities cannot issue a FASC-N
  - Attempts to emulate FASC-N will lead to collision
- Authentication Certificate
  - Non-Federal entities cannot satisfy FIPS 201 requirements
  - Federal PKI Common Policy only available to Federal entities

Enabling Trust - Identity Proofing

- Adhere to NIST Special Publication 800-63 Identity Proofing Requirements for E-Authentication Level 4:
- In-person appearance and verification of two independent ID documents or accounts, one of which must be a current primary government ID that contains the applicant's photograph and either an address of record or nationality
  - For example: Drivers license, Passport
- A new recording of a biometric of the applicant at the time of application.
  - Photograph
  - Fingerprints (for PIV interoperability)

Enabling Trust - Unique Identifier

- Leverage existing elements within the PIV data structure (as defined in SP 800-73) by utilizing the GUID
- Include a valid IPv6 address in the GUID component of the CHUID for use as a unique identifier with federal relying parties.
- Include the GUID in a subject-alt-name extension of the authentication certificate

Enabling Trust - Authentication Certificate

- Activate a PKI Digital Certificate for which a Federal Relying Party can establish a trust path.
- Therefore, the PKI Certificate issuer must have a relationship with the Federal PKI, and
- The Authentication Certificate's policy OID must chain to the FBCA at Medium-Hardware or better

*FBCA cross certification enforces the identity proofing requirements.

Summary

- This interoperability guidance is still a work in progress
- **We are establishing an opportunity for trust, but the final decision is up to the authorizing agent of the relying party**
- The Unique Identifier solution needs some final ‘tweaking’
  - How do we get the PACS to look in the GUID for the identifier?
- Initial guidance expected by mid-July